REMARKS/ARGUMENTS

The Claims rejected under 35 USC § 112, second paragraph

Claims 3-5 and 22 were rejected, the Examiner is alleging that claims 3 and 22 use the term "said encryption" without proper antecedent basis. That assertion is not quite correct. Those claims use the term "said encryption key" rather than just "said encryption" as asserted by the Examiner. Additionally, with respect to "said encryption key" it is respectfully submitted that there is sufficient antecedent basis for the use of that phrase in final sub-paragraph of claim 1 which refers to "an encryption/decryption key pair". It is noted that the Examiner has not objected to the later use in claim 1 of "said decryption key" and therefor it would seem that the use of "said encryption key" in claim 3 is perfectly consistent with such usage.

As to claim 22, "said encryption key" has antecedent basis in the "encryption/decryption key pair" of claim 19; later in claim 19 reference is made to the "IBE encryption key". Claims 22 and 23 have been amended to insert "IBE" before "encryption key" for consistency's sake.

Claims 10 and 27 were rejected, the Examiner alleging that claims 10 and 27 used the term "second key pair" without proper antecedent basis. Claims 10 and 27 have been amended to provide an antecedent basis for "second key pair".

Claims 33-35 were rejected, the Examiner alleging that claims 33-35 use the term "service provider" without proper antecedent basis. That assertion is believed to be in error. Kindly note the antecedent "service provider" in claim 33 which basically begins with "wherein the encrypted data is data encrypted by a service provider". That should suffice as an antecedent for the term.

<u>The rejections based on the prior art</u>

<u>Characteristics of IBE</u>

In identifier-based encryption, the data to be encrypted is encrypted using as encryption parameters:

- public data of a trusted authority;
- an encryption key string – this can be any arbitrary string typically selected by the encrypting party.

The private key is generated by the trusted authority using:

- the encryption key string;
- private data of the trusted authority, this private data being related to the public data of the trusted authority.

Using the public data of the trusted authority as an encryption parameter ensures that only that trusted authority can generate the private key needed for decryption.

Generally, the encryption key string will include conditions about who can receive the decryption key, and it is the responsibility of the trusted authority to check these conditions are satisfied before releasing the decryption key – this is what the trusted authority is being trusted to do.

<u>The Present Application</u>

In general terms, this case concerns delegating authority from the trusted authority that is normally responsible for generating the decryption key and controlling its release, to a (user) device. This way, after initial set up, only two parties need to be involved in an encryption/decryption transaction – there is

no longer a need to contact the trusted authority as its delegate is already present in a device of the decrypting party.

The problem is how to reliably delegate authority from the trusted authority. Effectively, the delegate (entity 25 in the Figure 3 embodiment of the invention) has its own public/private data just like a normal IBE trusted authority and is provided by the real trusted authority (entity 40) with the necessary data ('profile data') for checking the conditions in the encryption key string. However, to ensure that the delegate behaves properly, the profile data and the IBE private data of the delegate are locked away in the delegate (trusted computing mechanisms are used for this in the preferred embodiment) and are only accessible for use by the delegate:

> "under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment" (quoting claim 1).

The public data of the delegate is put in a certificate signed by the real trusted authority to reliably inform an encrypting party that that public data belongs to a genuine delegate of the trusted authority.

Claim 1 is couched in somewhat different terms to the above because what is conceptually going on is the establishment of a chain of trust based on a succession of public/private key pairs that are reliably linked to each other to form a chain.

There can be three or more key pairs in a chain and since claim 1 is written generically, there can be three or more key pairs in terms of that claim, the key pair at the start being the "starting key pair" and the key pair at the end being the "end key pair", while the key pair immediately before the end key pair being the "penultimate key pair". Other possible key pairs are not mentioned in

that claim. However, for specific exemplary chains, it is often easier to refer to the key pairs by their order number in the chain and thus:

- for a chain with THREE key pairs, reference can be made to first, second and third key pairs (the first key pair being the "starting key pair", the second key pair being the "penultimate key pair" and the third key pair being the "end key pair"); and
- for a chain with FOUR key pairs, reference can be made to first, second, third and fourth key pairs (the first key pair being the "starting key pair", the third key pair being the "penultimate key pair" and the fourth key pair being the "end key pair").

In the embodiment of Figure 3 of the present application, there are three key pairs in the chain as explained on page 17, lines 20-30:

> "The above-described embodiment of Figure 3 effectively provides trustable delegation by providing a chain of key pairs linked in a subversion-resistant manner. More particularly, and as illustrated in Figure 4, this chain comprises:
>
> - a first key pair 50 formed by the trusted authority's public/ private key pair, the private key being held in the cryptographic module 43 of the trusted authority 40;
> - a second key pair 52 formed by the IBE base key pair, that is, the public data N and the private data p,q, the latter being stored in the Protected Storage 27 of the trusted delegate entity 25; and
> - a third key pair 54 formed by the IBE encryption / decryption key pair, the decryption key being temporarily held in the entity 20."

The nature of the trustable links between the key pairs of the Figure 3 embodiment is explained in the passage from page 17, line 31 to page 18, line 16:

> "The link 51 between the first and second key pairs 50 and 52 is provided by the certification of the public data N using the trusted authority's private key…
>
> The link 53 between the second and third key pairs 52 and 54 is provided by the key generation process 28 which uses the private data

> p,q to generate the IBE decryption key – since the process 28 can only access the private data p,q and the profile data if it is executing in a benign environment, the service provider can trust this link …"

It is also important to note, as stated on page 18, lines 18-22:

> "It should be noted that the chain of key pairs 50-54 is incomplete at the stage immediately following the delegation of authority from the trusted authority 40 to the trusted delegate entity 25 (that is, at the end of phase [1] in Figure 3); this is because the final key pair – the IBE encryption/decryption key pair 54 has not yet been generated. This latter key pair is generated at each service request."

While the embodiment of Figure 3/4 embodiment has three key pairs and two trustable links in the complete chain, the embodiment of Figure 5 has four key pairs and three trustable links. Longer chains are possible as mentioned above.

Claim 1 is couched in terms of *"a yet-to-be completed chain of public/private cryptographic key pairs linked in a subversion-resistant manner"*. The chain starts with the key pair of the trusted authority (**'starting key pair'**) and has as its **'penultimate key pair'** the public/private data of the delegate device; the **'end key pair'** is the yet-to-be-formed IBE encryption/decryption key pair. An important feature is the **link** between the penultimate key pair and the end key pair:

> "this link being said key-generation process arranged to execute in said subversion–resistant operating environment on the device to generate said decryption key using said private data and the IBE encryption key and to make the generated key available for use …" [see claim 1]

Note that the 'end key pair' is not a recited feature of the claim, recalling that the chain is 'yet-to-be completed'.

Dependent claims 9 and 10 have been amended to refer to the number of key pairs which will exist in the "yet-to-be completed chain of public/private cryptographic key pairs". As can be seen, claim 9 now refers to three key pairs

in the yet-to-be completed chain of public/private cryptographic key pairs while claim 10 refers to four key pairs in that chain, which should help explain the terminology of these claims and make it even more clear why the penultimate key pair is the second key pair in claim 9 and the third key pair in claim 10.

The independent claims still active in this Application are:

1. **Method** of delegating key-provision authority from TA to a device via key-pair chain ending in IBE keys – here the chain is 'yet to be completed'

19. **Method** of controlling data access involving delegating authority from TA to a device via key-pair chain ending in IBE keys – here completion of the chain is attempted.

53. **System** for delegation of TA authority to a device via key-pair chain ending in IBC keys.

<u>The 35 USC 102 Rejections</u>

The Examiner relies on US 2004/0098589 (Appenzeller) which relates to a fairly standard IBE system but discloses the uses of multiple private key generators PKGs (equivalent to the trusted authorities of the present application). In particular:

- Each PKG has a public/private key pair (P,sP)/s (see paragraph [0042]);
- IBE encryption is carried out with public encryption key Q (identity of intended receiver) and the public data (P, sP) of the PKG (see paragraph [0057]);
- IBE decryption is carried out with private decryption key sQ generated by the PKG (see paragraph [0062]).

It should be noted that the private key of the PKG is referred to as "s" up to paragraph [0069] whereas from paragraph [0070] this key is referred to as "S"; the examiner has used "S" so the Applicant do likewise below.

The contribution of Appenzeller appears to be the provision of directory services for providing a sender associated with one PKG with appropriate public parameters to use when encrypting messages for a receiver that is associated with a different PKG.

In Appenzeller, clearly the PKGs must be trusted entities. The directory services may also be trusted (see paragraph [0083]) but if not, reliable public parameter information on the PKGs can be provided by a 'Certificate Authority 50' (Figure 5 and paragraph [0083]) which is a trusted entity.

Turning now to the Examiner's arguments on page 4 of the Official Action where he seeks to apply Appenzeller to claim 1, let us consider first the key pairs of claim 1 and then the link between the penultimate and end key pairs. In the following, quoted passages from claim 1 appear in italics.

First, note the claimed Key Pairs:

> *"**a starting key pair** formed by a public/private key pair of the trusted authority,"*

Examiner: "see at least, [0041]: the examiner notes the master secret S (e.g. master key) can be produced off site (e.g. trusted authority and is sent to the PKG"

Response: The Examiner has not clearly pointed out any <u>key pair</u> at all! The master secret 'S' is clearly used by the PKG 16 as its private key, its corresponding public key being (P, SP) – see paragraphs [0041] – [0043]. This corresponds to the teaching of Boneh and Franklin in the seminal paper referenced in paragraph [0039]. However, it is unclear whether the Examiner is trying to say that the starting key pair of claim 1 corresponds

to the private/public key pair of the PKG 16, or to the private/ public key pair of some other entity.

The Examiner does note that 'S' is a secret (and therefore presumably a private key) and can be provided by an unspecified off-site entity. Even if one accepts that, in the case of the master secret S being generated away from the PKG and then delivered to it as suggested in paragraph [0041], the entity generating secret 'S' must by implication be 'trusted', there is no suggestion in Appenzeller that 'S' is part of a key pair of this implied trusted entity.

A person of ordinary skill in the art would readily identify 'S' as the secret or private key of the PKG. Furthermore, Appenzeller clearly also considers the 'master secret' to belong to the PKG – see, for example, paragraph [0070]. Therefore, the only way Appenzeller can be read as disclosing *"a public/ private key pair of the trusted authority"* is by treating the PKG 16 of Appenzeller as the trusted authority of claim 1 and the key pair as [S / (P, SP)] which is, indeed, the correct view of Appenzeller (PKG 16 corresponds to the trusted authority of the the present application).

*"**a penultimate key pair** formed by public/private data, the private data being securely stored in the device for access only under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment,"*

Examiner "see at least, [0066]: the examiner notes a public key can identify the receiver and further the receiver has public parameter information P and SP maybe shared between a large number of potential recipients"

Comment: Again, the Examiner fails to point out a <u>key pair</u> but simply refers to the public key identifying a receiver. According to line 4 of the referenced paragraph [0066], this public key is "Q" - which is actually the public key part of the IBE encryption / decryption key pair, the corresponding private key being "SQ" referred to at line 14, para [0066]. According to claim 1, the IBE '*encryption / decryption key pair*' of claim 1 forms the '*end key pair*' . The Examiner makes reference to the public parameters P and SP; but as already noted, t<u>hese public parameters constitute the public key of the PKG and do not form a key</u>

<u>pair with the public key Q identifying the receiver (not least because P, SP and Q are all public and do not include anything that could be a private key of a public/private key pair)</u>.

an end key pair *to be formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme;*

Examiner: -

Comment: As already noted, the "*end key pair*" of claim 1 is not actually a recited claim feature, merely something that will exist at one end of the recited link (the other end being the "*penultimate key pair*").

From the foregoing, it can be seen that, at best, the Examiner has indirectly referenced two key pairs in Appenzeller, namely:

Key pair with private key S and public key P, SP;
Key pair with private key SQ and public key Q:

Rather than making assumptions regarding how the Examiner equates these key pairs to the key pairs of claim 1, it is probably simpler to note that Appenzeller really only discloses two key pairs (those noted above) whereas claim 1 refers to three key pairs (starting, penultimate and end key pairs, though the "end key pair" of claim 1 is not a recited claim feature). Therefore, for Appenzeller to anticipate claim 1 with its starting and penultimate key pairs, there is only one reasonable mapping:

Appenzeller key pair S / (P,SP) allegedly corresponds to the "starting key pair" of claim 1; and

Appenzeller key pair Q / QP allegedly corresponds the "penultimate key pair" of claim 1.

But, in reality, the two key pairs of Appenzeller apparently map to the penultimate and end key pairs of Claim 1 and Appenzeller has no key pair corresponding to the "starting key pair" of claim 1.

The Requirement of a Link between the Penultimate and End Key Pairs:

*"**a link between the penultimate key pair and an end key pair** to be formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme; this link being said key-generation process arranged to execute in said subversion–resistant operating environment on the device to generate said decryption key using said private data and the IBE encryption key and to make the generated key available for use."*

Examiner: "see at least, [0039]: the examiner notes an identity based encryption scheme in which private keys (e.g. see [0047]) maybe generated based on the identities of the users and [0057] and [0065]: the examiner notes the receivers equipment uses values of the private key for decryption."

Comment: The private key referred to by the Examiner is clearly the IBE decryption key SQ discussed above. Does this mean that the Examiner considers the IBE encryption/decryption key pair Q, SQ to be the "*end key pair*" of claim 1? As discussed above, this cannot be the case – or if it is, Appenzeller does not show two other key pairs as required by the '*starting*' and '*penultimate*' key pairs of claim 1.

The Examiner appears to make no attempt to identify the required "*key-generation process*" providing a "*link between the penultimate key pair and an end key pair*" except for his reference to 'decryption'.

According to claim 1, the 'link' is said to be:

"said key-generation process arranged to execute in said subversion–resistant operating environment on the device to generate said decryption key using said private data and the IBE encryption key and to make the generated key available for use."

In other words, the claim 1 "*link*" is <u>the process that generates the IBE decryption key</u> and not the decryption process. The process that generates the IBE decryption key is, in Appenzeller, the process used by the PKG to generate SQ. This process uses S from the Appenzeller key pair S / (P,SP) and generates

SQ of the Appenzeller key pair Q / SQ; the process thus links the two key pairs of Appenzeller – however, if this key generation process were to anticipate the link of claim 1, it would require:

- Appenzeller key pair S / (P,SP) to be the Claim 1 "*penultimate key pair*"; and
- Appenzeller key pair Q / QP to be the Claim 1 "*end key pair*".

This returns us to the situation that there is no key pair of Appenzeller corresponding to the "*starting key pair*" of claim 1. So claim 1 is clearly not anticipated by Appenzeller..

The inevitable conclusion is that Applicant cannot find any disclosure in Appenzeller the inter-relationship of key pairs and links that is set out in claim 1.

A Further Difference is noted:

It should also be noted that Appenzeller apparently has nothing to say about the following feature of claim 1:

"*the private data being securely stored in the device for access only under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion–resistant operating environment*"

While private data (a.k.a private key) is likely to be securely stored in an entity (the claim 1 "device"), there is nothing in Appenzeller about a different entity (the claim 1 "trusted authority") specifying any access conditions and certainly not that those access conditions are that "*a specific key-generation process*" must be "*running in a subversion–resistant operating environment*" of the device.

The foregoing novelty arguments advanced above in respect of claim 1 also apply to claims 19 & 53.

Withdrawal of the rejections and allowance of the claims are respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, then the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136 (a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being transmitted electronically to Commissioner for Patents on

24 October 2008
(Date of Transmission)

Lonnie Louie
(Name of Person Transmitting)

/Lonnie Louie/
(Signature)

24 October 2008
(Date)

Respectfully submitted,

/Richard P. Berg 28145/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile